Across Heterogeneous Wireless Networks

Hong Chen
Faculty of Computer Science
University of Twente
The Netherlands
chen@cs.utwente.nl

Miroslav Živković, Dirk-Jaap Plas
Lucent Technologies
Bell Labs Advanced Technologies
The Netherlands
{mzivkovic, dplas}@lucent.com

Abstract - **With the increasing number of mobile and wireless networks that are deployed, the handovers between these systems take place more often. In order to provide end-users with uninterrupted access to services, support for fast handover is essential. One of the pre-requisites of a fast-handover is transparent end-user authentication. In this paper we address end-user authentication at network level. We focus on providing transparent end-user authentication across UMTS and WLAN network technologies. The end-user should be unaware of the underlying network technologies when it comes to authentication. We describe two solutions. For the first solution, authentication is based on the authentication mechanism of the UMTS network. This authentication relies on the shared secret between the UMTS SIM (USIM) card and the end-user's home network. The authentication in the second case is based on multiple authentication mechanisms; it overcomes the issue of authentication differences in UTMS and WLAN networks.**

Keywords: UMTS, WLAN, Authentication, USIM, PEAP.

I. INTRODUCTION

The next generation of wireless networks will adopt an architecture that combines different networks in order to obtain wider area of coverage, higher data throughput, and better frequency reuse. While the wide coverage of technologies such as UMTS provides the end-user with always-on capability, technologies such as WLAN can provide hotspot data services as well as voice services at higher rates than UMTS. This will encourage end-users to connect to WLAN whenever possible to access their high bandwidth services.

The small coverage of WLAN makes handovers happen frequently for mobile users. These handovers can be either between WLANs or between WLAN and other access technologies, e.g. UMTS. In order for the end-users to achieve uninterrupted network access to services, fast-handover support is essential. One of the pre-requisites of fast-handover is transparent end-user authentication. The authentication mechanisms that are currently used in UMTS and WLAN are different. These mechanisms are developed separately, and were not designed to interoperate.

In this paper we describe the solutions that enable transparent end-user authentication across different wireless access technologies; the benefit of transparent authentication is seamless roaming experience for the end-user. We will start by providing a brief summary of the authentication mechanisms of UMTS and WLAN in Section II. Section III describes the two solutions we propose to provide transparent end-user authentication. A short analysis of solutions will be provided in Section IV. Experiences from implementation of one of the solutions are described in Section V. Finally, the conclusions and directions for future work are presented in Section VI.

II. UMTS AND WLAN AUTHENTICATION MECHANISMS

This section provides a brief summary of the authentication mechanisms that are used in both UMTS and WLAN networks.

The UMTS security mechanisms (including authentication) are specified by the 3rd Generation Partnership Project (3GPP) [1]. They are based on three principles [2]:

- 3G security will build on the security of second generation systems
- 3G security will improve the security of second generation systems
- 3G security will offer new security features and will secure new services offered by 3G

Authentication and Key Agreement (AKA) is an important feature of the UMTS system. Authentication of the end-user in UMTS [3] is performed in a similar way as authentication in GSM [4] and both GSM AKA and UMTS AKA are based on challenge-response mechanism. The main difference is that UMTS AKA enables mutual authentication: end-user towards the network, as well as authentication of the network towards the end-user.

In short, the authentication flow is as follows [3]:

- A master key is shared between the end-user's UMTS SIM (USIM) and the home network.
- The Visiting Location Register (VLR) or Serving GPRS Support Node (SGSN) authenticates the terminal by sending an authentication request to the Home Location Register (HLR) that answers with a set of authentication vectors.

- The VLR/SGSN sends an authentication request: including a randomly generated number (RAND) and AUTH to the terminal.
- The terminal authenticates the network from the request generated by the network using its own key.
- The terminal sends the response to the VLR/SGSN. The VLR/SGSN is then able to compare user response RES with the expected response XRES (thus authenticating the terminal to the network)

The master key is never transmitted and the end-user has no knowledge of it. At the same time during the mutual authentication, keys for encryption and integrity checking are derived.

On the other hand, in enterprise WLAN environments, authentication is commonly realized by a statically configured access list of allowed Medium Access Control (MAC) addresses, combined with static Wired Equivalent Privacy (WEP) key that is only distributed to employees. The shortcomings of WEP are analyzed in more detail in [5]. For the public environment another authentication method for WLAN is available: Universal Access Method (UAM) which is described in de-facto standard [6]. Upon accessing a public WLAN an end-user is presented a web page where he or she must enter a username (including the provider's domain) and a password before being allowed to use the Internet. This de-facto standard again does not address end-user privacy, and prevents seamless roaming by requiring user interaction. UAM or web-based authentication in general does seem to become the most widely deployed authentication method for the coming period, until better alternatives are adopted.

In addition, there exists a feasible security solution for WLAN networks, based on a standard security framework defined by IEEE 802.1x [7]. This framework supports dynamic WEP keys, ensuring a sufficiently secure encryption to protect the privacy of mobile users. In addition, through the Extensible Authentication Protocol (EAP) [8] IEEE 802.1x supports various methods to authenticate the end-user (or his device) for use in a WLAN. The EAP Message Digest (MD) variant that uses a username and password (EAP-MD5 [8]) prevents seamless roaming, unless the end-user has predefined username and password. A more secure solution (EAP Transport Level Security, EAP-TLS) is based on a digital certificate containing the user's credentials [9]. The certificate can be installed on the device or on a smart card or token.

Protected Extensible Authentication Protocol (PEAP) [10] is a new member of the family of EAP protocols. PEAP uses TLS to create an encrypted channel between an authenticating PEAP client and a PEAP authenticator, such as an Authentication Service (AS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols.

To enhance both the EAP protocols and network security, PEAP provides:

- Protection for the EAP method negotiation that occurs between client and server through a TLS channel.
- Wireless clients with the ability to authenticate the AS. Because the server also authenticates the client, mutual authentication occurs.
- Protection against the deployment of an unauthorized wireless access point (AP) when the EAP client authenticates the certificate provided by the AS server. In addition, the TLS master secret created by the PEAP authenticator and client is not shared with the access point. Because of this, the access point cannot decrypt the messages protected by PEAP.
- PEAP fast reconnects, which reduces the delay in time between an authentication request by a client and the response by the server, and allows wireless clients to move between access points without repeated requests for authentication. PEAP offers fast re-authentication capability that supports efficient roaming between access points in WLAN.

III. Authentication Solutions in Heterogeneous Networks

This section introduces two authentication solutions for UMTS networks and WLANs. One solution is based on the USIM and the other solution provides a way to integrate different authentication mechanisms in UMTS and WLAN. For both solutions, we first provide the assumptions, followed by the authentication procedure. A comparison of the two solutions is given in section IV. We assume the end-user's mobile terminal (MT) has dual or multiple access network interfaces that enable the terminal to access heterogeneous networks. There is a mechanism in the MT to decide which access network to attach to. In both solutions, the MT supports mobile IP (MIP). MIP is required to enable seamless roaming on IP level.

A. UMTS SIM (USIM) based solution

This solution is based on the authentication mechanism of the UMTS network. A generic solution using a USIM authentication mechanism in both UMTS networks and an IP based network can be found in [11]. Our solution described here is tailored to an architecture that consists of IEEE 802.11 based WLANs and UMTS networks.

1) Assumptions

- The UMTS network and WLANs use the same authentication server (AS) located in the UMTS network. Each AS has digital certificate issued by a Certificate Authority (CA). The CAs can be different for the authentication servers in different UMTS networks.
- The MT is always connected to the UMTS network.
- The MT needs to obtain the public key of the serving AS if it wants to switch to the WLANs affiliated to it. The key can be passed to the MT by the UMTS network during a mutual authentication, either with the home network or with the visiting network.

- The WLANs are located within the range of UMTS networks they are affiliated with, which assures that a MT has the public key to validate the AS of a WLAN.
- The MT supports the PEAP, including our USIM extension.

2) Authentication procedure

For this solution we have developed a new PEAP based authentication method: PEAP-USIM. The reasons to choose PEAP instead of EAP are the additional security features as described in Section II.

The validation of the AS is done through the validation of its digital certificate. The authentication of the MT is done through the P-TMSI and CK which are carried on the USIM.

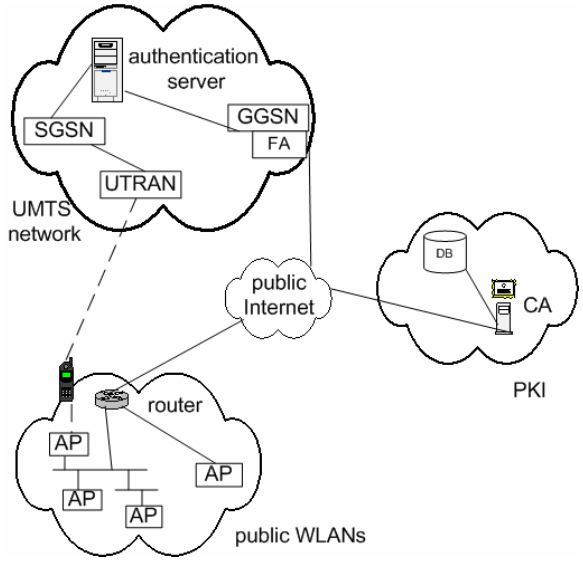

Figure 1. The PEAP--USIM based solution

The mutual authentication procedure to a WLAN is as follows (see also Figure 1):

a) The AS sends a PEAP/Start packet, which is an EAP-Request packet with EAP-Type=PEAP, the Start (S) bit set, and no data. The initial clear text identity exchange is omitted to protect the identification of the end-user from disclosure. The AP acts as a proxy and Network Access Server (NAS) between the MT and the AS.

b) The MT sends an EAP response packet with EAP-Type=PEAP. The data filed of the packet contains the information needed to setup a TLS link.

c) The AS sends its certificate to the MT while setting up the TLS secure link. The MT validates the certificate using the public key it received from the UMTS network during its association with current UMTS network. If the authentication succeeds, the procedure continues, as the secure link has been set up.

d) The MT and AS negotiate and agree to use PEAP-USIM authentication method.

e) The AS sends a RAND to the MT. The MT processes the challenge using the CK in its USIM and sends the result to the AS.

f) The AS verifies the MT by looking up the P-TMSI list and finds the CK in the VLR of the end-user. It then carries out the same calculation as the MT did using the RAND and CK and compares the results. (According to the assumptions, hotspots deployed by service provider A are within the range of UMTS networks of service provide A, the AS need only to check the data in its local VLR.

g) If the authentication succeeds, the AS sends an authentication success message to AP, which will enable its controlled port for the MT's MAC address and enables a WEP key.

h) The MT obtains a new local IP address which will be used in the WLAN. The new local IP address will be registered at home agent.

Because of the "always-on" service in UMTS network, the end-user can quickly switch back to the UMTS network. The MT only needs to register the local IP address assigned by the UMTS network at the home agent. It does not need to authenticate itself again to the UTMS network.

For the WLANs owned by enterprises or individuals that have their own authentication mechanism, the authentication method can be negotiated after the TLS channel has been set and they need not to support this PEAP-USIM method.

B. Solution using multiple authentication mechanisms

In this solution the UTMS networks and WLANs use different authentication mechanisms. Authentication in UMTS network is based on USIM. Authentication in WLANs is based on digital certificates. The authentication mechanisms for WLAN such as 802.1x and EAP-TLS support mutual authentication between MT and AS. The AS has Internet access during the EAP authentication; it is capable of following a certificate chain to verify a peer's identity. However, the MT does not have a connection to the Internet before the authentication succeeds. As the MT stays offline, in order to validate the certificate of an AS, the MT needs to hold public keys of different CAs, as well as the certificate revocation list (CRL) of each CA. This may be difficult for the MT, which has limited storage space. As the number of CA grows and when there is a certificate chain the situation becomes worse. The solution relies on the always-on ability enabled by the UMTS network. It means we can use the UMTS link to access to the Internet and validate the certificate of an AS when necessary.

1) Assumptions

- The UMTS networks and WLANs are managed by different operators. They use different authentication servers.
- The UMTS and WLAN network operators have established roaming agreements. The MTs are always

connected to the UMTS network because of its wide coverage.

- Every MT and each WLAN AS have a digital certificate issued by a CA. The CAs that issue the certificates can be different. The digital certificates are used during mutual authentication.
- The WLANs lie within the coverage of a UMTS network.
- MT supports PEAP with our proposed extension.

2) Authentication procedure

The authentication of a WLAN is based on PEAP, where the certificate of MT could be sent before the TLS secure connection is set up so that the AS can authenticate the MT. However, in order to protect end-user identity from being sent in clear text, this is not done. The MT certificate is only sent after the TLS connect has been setup. For this solution, we define a new PEAP based authentication method: PEAP – Certificate.

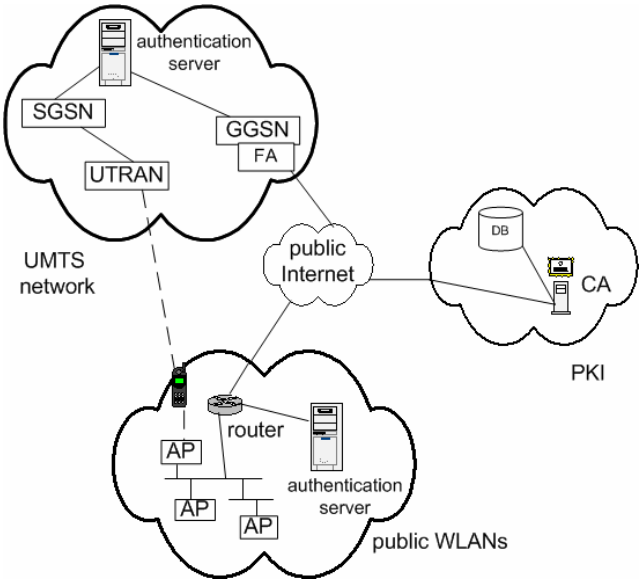

Figure 2. Solution using multiple authentication mechanisms

When a MT needs to switch from a UMTS network to a WLAN, the authentication begins and the procedure is described below (see also Figure 2):

a) The AS sends a PEAP/Start packet, which is an EAP-Request packet with EAP-Type=PEAP, the Start (S) bit set, and no data. The initial clear text identity exchange is omitted to protect the identification of the end-user from disclosure. The AP acts as a proxy and NAS.

b) The MT sends an EAP response packet with EAP-Type=PEAP.

c) AS sends the certificate to the MT while setting up the TLS secure link. The mobile terminal validates the authentication server. Through the UMTS Internet connection, it is capable of following a certificate chain or verifying whether the certificate has been revoked.

d) MT sends an EAP response to set up the TLS link. The MT's digital certificate is not sent in this message.

e) After the TLS link has been set up, the AS and MT negotiate to use PEAP-Certificate method. The MT then sends its certificate to the AS. Because AS is on the Internet, it can always connect to the CA to validate the certificate of the MT.

f) If the authentication succeeds, the AS sends a authentication success message to AP, which will enable its controlled port for the MT's MAC address.

g) The MT obtains a new local IP address that will be used in the WLAN. The new local IP address will be registered with the home agent.

Because of the "always-on" service in UMTS network, the end-user can quickly switch back to the UMTS network. The MT only needs to register the local IP address assigned by the UMTS network at the home agent, and does not need to authenticate itself again to the UTMS network.

IV. COMPARISON OF THE SOLUTION

The first solution, based on the UMTS authentication mechanism, is especially useful when the UMTS network operator wants to deploy WLANs as an augment to the cellular network. The network operator can reuse the existing infrastructure for authentication. Roaming users can easily be allowed to use WLANs that are affiliated to visited UMTS networks, based on roaming agreements. The end-user information is transferred from the home network to the visited network during the authentication of normal UMTS terminals. The end-user can switch to the WLANs relatively fast, since the secure association is always done locally. The disadvantage of this solution is that the WLANs must lie within the range of the UMTS network they are affiliated with. Otherwise, the end-user won't acquire the public key to validate the authentication server.

The second solution, based on multiple authentication mechanisms, is more applicable when different network operators deploy UMTS and WLAN networks, possibly using different authentication mechanisms. Currently, the number of WLAN hotspots is increasing, providing Internet access in public places, such as bars, hotels and train stations. The solution we propose can easily integrate the existing and emerging wireless network technology, such as UMTS and WLAN. Our solution requires minor extensions of the existing authentication protocols. However, some additional software at the mobile terminal is required. Every mobile terminal should also possess a digital certificate. Although server certificates are common today, the usage of client certificates is not yet widely adopted.

V. IMPLEMENTATION

The second solution has been validated as part of the 4GPLUS project [12]. The research in the 4GPLUS project is focused on the development of a service platform for beyond

3G environments. The service platform hides the complexity and the heterogeneity of the underlying networks to both the end-user and the service provider. The service platform provides mobility management across different types of access networks, therefore providing a seamless roaming experience to the end-user. This includes the provisioning of transparent end-user authentication.

Reference [13] provides a high-level overview of the integrated security architecture we applied within 4GPLUS project. Due to the absence of operational UMTS networks, GPRS – for which the authentication mechanisms are comparable to UMTS – is used. The service platform acts as an authentication server that takes care of the authentication for different network domains. The service platform can integrate the different authentication mechanisms used within the different domains and can provide the end-user with one subscription for all these networks. For the GPRS network, SIM based authentication is used. When the end-user roams to WLAN, this is detected by the mobile terminal, the end-user is authenticated and the network interfaces are re-configured without any service interruption or end-user involvement. The current implementation illustrates how a loosely coupled approach can be used to provide transparent end-user authentication across networks that are using different authentication mechanisms

VI. Conclusions and Future Work

In this paper, we have described two solutions to provide transparent end-user authentication across heterogeneous wireless networks, in particular UMTS and WLAN. The first solution is based on the authentication mechanisms of the UMTS network. This solution is very suitable for operators who want to deploy WLAN as an augment to their UMTS networks. It applies the authentication mechanism used in the UMTS network to WLAN technology. Using a security mechanism in another environment than it initially has been designed for, usually introduces security vulnerabilities. Further research is required to identify these vulnerabilities by performing a detailed risk analysis and a detailed analysis of the security mechanisms.

The second solution is based upon multiple authentication mechanisms. This solution is aimed at the situation where different service providers deploy UMTS and WLAN networks. Both solutions are based on the PEAP protocol specification of the IETF.

The beyond 3G environment not only consists of UMTS and WLAN networks; it contains more subsystems, such as satellite networks, wireless local loops and so on. Future study on transparent end-user authentication can be extended to these subsystems.

In addition, service providers in the future can provide full coverage and seamless connection to the end-users, by establishing agreements with other access network operators. End-users can then select the best networks available to them. An interesting research topic is to see how profile information can be used to do this automatically.

Acknowledgments

We would like to thank Gerard Hoekstra, Ko Lagerberg and Harold Teunissen from Bell Labs Advanced Technologies EMEA for their contribution to this paper.

Elements of the work described in this paper are part of the research project called 4GPLUS [12]. This project is supported in part by the Dutch Freeband Impulse Program on Telecommunication Applications (http://www.freeband.nl/) and is co-funded by the Dutch Ministry of Economic Affairs.

References

[1] 3rd Generation Partnership Project, http://www.3gpp.org.

[2] 3GPP Technical Specification "TS 33.120, Security Principles and Objectives", March 2001.

[3] 3GPP Technical Specification "TS 33.203, Access Security for IP-based Services", June 2003.

[4] 3GPP Technical Specification "TS 03.20 V8.1.0, Security related network functions", October 2000.

[5] Nikita Borisov, Ian Goldberg, David Wagner, "Security of the WEP Algorithm", http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[6] Wi-Fi Alliance, "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming", version 1.0, http://www.wifialliance.org/opensection/downloads/WISPr_V1.0.pdf, February 2003.

[7] IEEE 802.1x "Port Based Network Access Control", http://www.ieee802.org/1/pages/802.1x.html, June 2001.

[8] IETF, RFC 2284, "PPP Extensible Authentication Protocol (EAP)", http://www.ietf.org/rfc/rfc2284.txt, March 1998.

[9] IETF, RFC 2716, "PPP EAP TLS Authentication Protocol", http://www.ietf.org/rfc/rfc2716.txt, October 1999.

[10] IETF, Internet Draft, "Protected EAP Protocol", http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-06.txt, March 2003.

[11] Juha Salvela, "Access Security in Third Generation Mobile Networks', Proceedings of the Helsinki University of Technology Seminar on Network Security, fall 2000.

[12] 4GPLUS Project, 4th Generation Platform Launching Ubiquitous Services, http://4gplus.freeband.nl.

[13] Jeroen van Bemmel, Harold Teunissen, Gerard Hoekstra, "Security Aspects of 4G Services", published at Wireless World Research Forum #9, http://www.wireless-world-research.org, July 2003.